



This guide is valid for Open-Mesh/Cloudtrax using firmware-ng or robin-mesh firmware

To integrate Chillifire Hotspots with Open-Mesh networks first of all you have to have an account their mesh network control panel on <https://www.cloudtrax.com> as much as you need an account with Chillifire. You can create a free Chillifire account on <http://www.chillifire.net>.

There is nothing special to consider in the setup of the Chillifire account, which you can configure any way you like to, free, pay-per-use, voucher based, online-payment, your own logo, colour scheme etc. However, the open-mesh/cloudtrax account has to be setup in a certain way to work with your Chillifire account:

General Tab

There is nothing much to consider on this tab although we recommend to un-check 'Disable Limited View' and to check 'Disable Internet Check'. We also recommend you set the 'TX Power' field to 'Use Country Settings' to avoid any issues within your regulatory jurisdiction. Other than that just enter your relevant contact details on this screen and press 'Update Network Settings' at the top of the screen.

The screenshot displays the 'General Settings' tab of the Chillifire web interface. The interface includes a navigation bar with 'Home', 'Edit Network', 'Network Status', and 'Log Out' options. Below the navigation bar, there are tabs for 'General', 'SSID #1', 'SSID #2', and 'Advanced'. The 'General Settings' section is active and contains various configuration fields and checkboxes. On the right side, there are several informational boxes providing details for each field. The fields include: 'Nodes' (with an 'Add / Edit Nodes' button), 'Users' (with 'Show / Block Users' and 'Vouchers' buttons), 'Map Overlay' (with 'Choose File' and 'Submit' buttons), 'Network Location' (set to 'Wellington, New Zealand'), '* Login ID' (set to 'chillifire'), 'Time Zone' (set to 'Pacific/Auckland'), 'Country' (set to 'New Zealand'), 'TX Power' (set to 'Use Country Setting'), '12hr (am/pm) time' (checked), 'Display Name' (set to 'chillifire'), '* Password' (masked with asterisks), '* Lobby Password' (empty), 'Disable Limited View' (unchecked), 'Disable Internet Check' (checked), '* Email' (set to 'contact@chillifire.net'), 'Notification Email' (set to 'open-mesh@chillifire.net'), 'Email Alerts' (checked), and 'Network Notes' (empty text area). The right side of the interface contains several informational boxes: 'Add nodes to your network and edit their name or description.', 'Show all users and their 24-hour usage and optionally block their access to the network. Vouchers let you create specific login codes for users. See Using Vouchers to Control Access for more information.', 'Overlay an optional floorplan or other image on the Map. Landscape images/floorplans work best as they will be stretched to fit the map. Maximum size is 75KB.', 'The address used to center the overlay image on the map.', 'Login ID for this network. You can rename networks by changing the name here.', 'The timezone for your network.', 'The regulatory domain which sets maximum power.', 'Manually set the TX Power for APs on this network. Can be used to reduce power on dense indoor networks with high power devices such as the OMDP. (Requires firmware NG r360 or later.)', 'Check to display time in 12 hour (am/pm) format.', 'The name to use on reports and the splash page. If left blank, the Network name will be used.', 'Administrator password for this network. Must not be empty.', 'Lobby Assistant password for this network. Logging in with this password on lobby.cloudtrax.com will display the create voucher page. All other edit access will be denied.', 'Check to prevent a password-free limited view of the network status. The password will still be required to change any network settings.', 'Keep the wireless network up in the event an internet connection is lost.', 'Your email in case we need to contact you. We will not share this with others.', 'Separate multiple email addresses with spaces. Outage notifications will be sent to these addresses if alerts are checked below.', 'If checked, send email alerts hourly. Alerts will only be sent once for each node. If you receive multiple alerts for the same node, then it came back up and went down again.', and 'Enter any unique notes for this installation you'd like to be able to refer to later.'



SSID #1 Tab

This screen sets up your mesh network's connection to the hotspot system, and thus is the centre point of your setup:

Make sure the 'Hide' field is NOT checked, so potential customers can find the hotspot.

We recommend you the same SSID for all mesh network nodes, so your users can roam between routers. To enable this put your hotspots name into the 'Network Name' field and un-check the 'Use Node Name' field. The 'Network Name' must be less than 32 characters and should not contain any characters other than letters, number, spaces, underscores and dashes.

Do not set a 'WPA Key' and do not check the 'WPA2 Only' field.

Choose 'Chillispot AAA' and select 'Manual' settings.

Select the 'RADIUS Server 1' setting according to you location. Choose 'radius 06.chillifire.net' if you are located in the Americas, 'radius04.chillifire.net' if you are located in the Europe, Africa and the Near East, and 'radius 02.chillifire.net' if you are located in the Australasia. Choose a different location's radius server for the 'RADIUS Server 2'.

'RADIUS Secret' must be set to '6Y4n8fW5tGTavrGm'.

'RADIUS NASID' must be set to the name of your Chillifire account (Chillidemo in this example).

The screenshot shows the 'SSID #1' configuration page in the Chillifire web interface. The page has tabs for 'General', 'SSID #1', 'SSID #2', and 'Advanced'. The 'Public SSID' section is active. It contains several input fields and checkboxes. The 'Network Name' is set to 'Chillifire_Hotspot'. The 'WPA Key (Password)' field is empty. The 'Captive Portals' section has 'Chillispot AAA' selected. The 'RADIUS Server 1' is 'radius02.chillifire.net' and 'RADIUS Server 2' is 'radius04.chillifire.net'. The 'RADIUS Secret' is '6Y4n8fW5tGTavrGm' and 'RADIUS NASID' is 'Chillidemo'. The 'UAM Server' is 'https://login02.chillifire.net', 'UAM URL' is '/hotspotaccess.php', and 'UAM Secret' is '5hHrC4US7xGyE.B'. The 'Allowed Domains' field is empty. There are also checkboxes for 'Hide', 'Use Node Name', 'WPA2 Only', and 'ChilliSpot Compatible'. On the right side, there are several informational boxes with text and links.



For the 'UAM Server' again choose the right server for your locality for best performance:

'https://login06.chillifire.net' if you are located in the Americas, 'https://login04.chillifire.net' if you are located in the Europe, Africa and the Near East, and 'https://login02.chillifire.net' if you are located in the Australasia.

'UAM URL' must be set to '/hotspotaccess.php'.

'UAM Secret' must be set to '5hHrC4US7xGxyE.B'.

You can leave 'Allowed Domains' blank if you do NOT intend to sell hotspot access only. In that case only add domains to the field, separated by commas, for such domains that you want users to have access without needing to login on to the hotspot. This could be promotional pages or your business homepage to give but some examples. IF you DO intend to sell hotspot access online you MUST add the following string to the allowed domain field:

paypal.com, paypalobjects.com, paypal-metrics.com, 112.2o7.net, moneybookers.com, skrill.com, omdrc.net, verisign.com, amadesa.com, 2checkout.com, thawte.com, securecode.com, adyen.com, paysafecard.com, mycardsecure.com, mixpanel.com, payfast.co.za, hittail.com, mbsvr.net, mxpnl.com, chillifire.net, secure5.arcot.com, cap.securecode.com, seal.verisign.com, seal.entrust.net, i1.mbsvr.net, api.recaptcha.net, paypalssl.doubleclick.net, mp.apmebf.com, altfarm.mediaplex.com, images.scanalert.com, seal.godaddy.com

Note: If you cut and paste the content from this PDF document please make sure that line breaks are removed.

The field 'ChilliSpot Compatible' must be checked.

Save settings by clicking on press 'Update Network Settings' at the top of the screen.



SSID #2 Tab

Only enable this second SSID, if you want to offer a free access to the Internet, which bypasses the Hotspot, but requires a pre-shared key (PSK), i.e. a password.

If you enable this feature make sure the fields 'Bridge' is not checked.

If you want the Ethernet jack on the OM2P or other devices with more than one Ethernet jack to be hotspot controlled then make sure 'Wired Clients' is not checked. If you do check the and 'Wired Clients' field the Ethernet jack will bypass the hotspot and gain any device connected to it free access to the Internet.

You must give this non-Hotspot network a name (Private_Network in this example) and set a Password (PasswOrd in this example).

The screenshot shows the 'Private SSID' configuration page in the Chillifire web interface. The 'Enable' checkbox is checked, and the 'Update Network Settings' button is visible at the top right. The 'Network Name' field contains 'Private_Network' and the 'Password' field contains 'PasswOrd'. The 'Wired Clients' checkbox is unchecked. The 'WPA-Enterprise Server' and 'WPA-Enterprise Port' fields are empty. The 'VLAN Tag' field is also empty. The right side of the page contains several informational callouts:

- Uncheck to disable this access point.
- Check to Hide this access point's name (SSID).
- Check to bridge SSID#2 with the LAN and disable NAT. This lets your LAN or internet modem assign all client DHCP addresses and gives clients access to LAN resources. Requires [Firmware NG](#).
- Check to have clients who connect via Ethernet use these SSID#2 settings. (If unchecked, Ethernet clients use SSID#1 settings). Requires [Firmware NG](#).
- The SSID to use to connect to this access point. Check the box below to use each node's name for its SSID instead ("secure" will be appended). Requires [firmware NG](#).
- WPA Key: Leave blank for an open network. KEYS MUST BE 8 CHARACTERS OR LONGER. WPA-Enterprise: Enter your RADIUS server password here & the server IP & (optional) port below.
- IP address of your 802.1x (WPA-Enterprise) RADIUS server. Requires [Firmware NG](#).
- Port # of your 802.1x (WPA-Enterprise) RADIUS server if not the standard port 1812. Requires [Firmware NG](#).
- Optional Tag for this SSID (allowed values are 2-4094). Requires [Firmware NG](#). Must be used a with 802.1Q compatible switch. Do not use with standard switches/routers.

Leave 'WPA Only' and all other fields on this page unchecked and empty.

Save settings by clicking on press 'Update Network Settings' at the top of the screen.



Advanced Tab

Set 'Root Password' to a secure password known only to you.

'Gateway LAN Block', 'Access Point Isolation', and 'Block Alien Nodes' must all be set.

Leave the channels unchanged, unless you have a lot of interference for other Wi-Fi routers on the same or on close channels.

'Disable Automatic Upgrades', 'NG firmware', and 'Test Firmware' should be unchecked unless you are an advanced open-mesh user and know what you are doing.

'SMTP Redirect' is useful to populate with your ISP's own SMTP server's IP address.

'Alternate Nameserver IP' can either be 8.8.8.8 for Google DNS, or alternatively you can link a service like Open DNS, or simply link you ISP's own DNS server for fast performance.

Leave 'Local Domain' and 'Alternate Dashboard' blank.

The most important setting on this page is the 'custom.sh Server' which MUST be set to 'support.chillifire.net/downloads/openmesh/'

'Enable custom.sh' MUST be checked.

Save settings by clicking on press 'Update Network Settings' at the top of the screen.



Adding Mesh Nodes to the Network

You'll be taken to the General Settings tab of the Edit Network page. On the top of the "Edit Network" page is an "Add/Edit Nodes" button. Click it.

A Google map, centred on the address you entered when you created the network, will appear in a popup. You can often (depending on location) click the "Satellite" view button and zoom in for a closer look. Click the map where you want to add your first node.

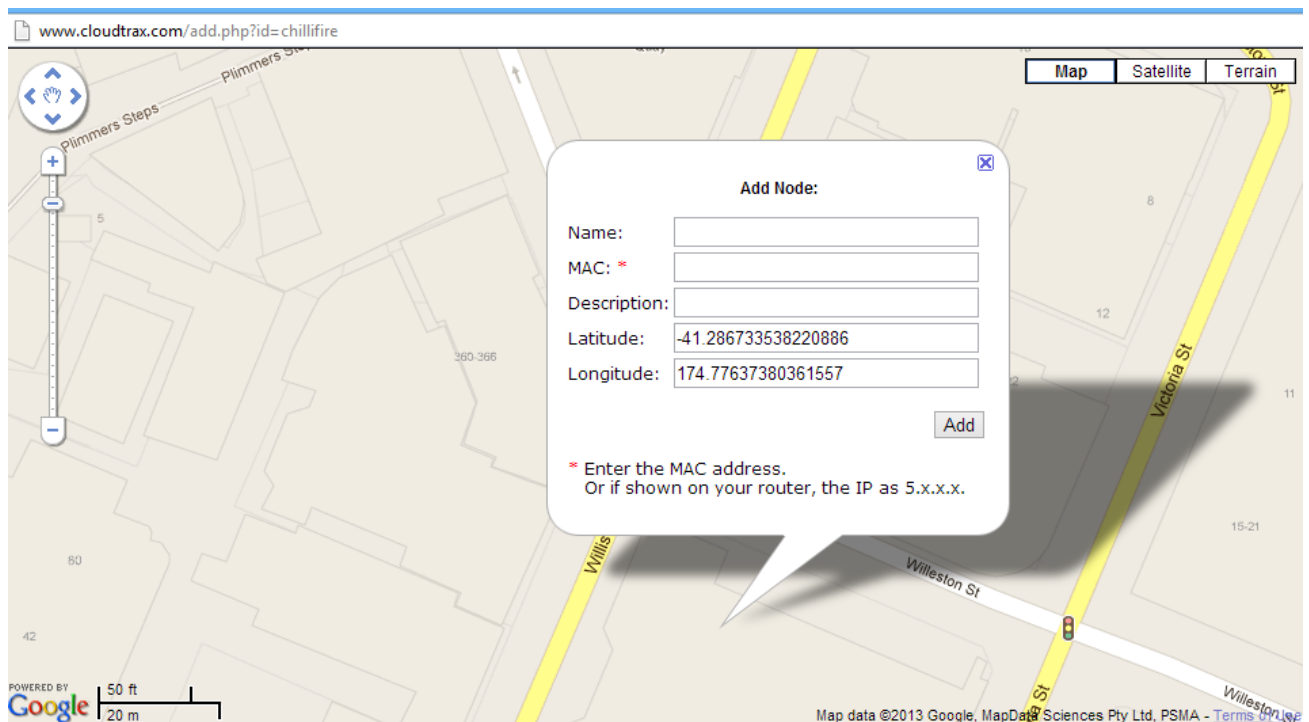
Next, you'll see a dialogue similar to the one on the right. Fill in the following information:

Name: Enter a name for this node. This name is used to reference its location and will be displayed in reports. It does not affect users.

MAC address: A MAC address is a sequence of 12 numbers and the letters A-F often separated by colons (e.g. 00:02:6F:8A:B2:6E). This can be found on a label on the bottom of the router and on the side of the product box. For the MR500, there are 3 MAC addresses shown, and you want to enter the one on the top, listed as the "WAN MAC."

Description: You can enter optional descriptive text that will be shown on the reports. This is typically used to keep notes on where the node is installed, etc.

Click "Add" and repeat the process for each additional node.





Installing the Nodes

Once your nodes are added to CloudTrax, it's time to install them.

First, connect your Gateway unit to the Internet with an Ethernet cable. This can be plugged in directly to your high-speed modem (if it has a single Ethernet port, power cycle it first), or it can be fed from a router or switch. If it can get an Internet connection through the cable, it'll connect to CloudTrax. Once the Ethernet cable is plugged in, connect power.

Next, plug in additional nodes as either gateways (connected to Ethernet) or repeaters, connected only to power.

To ensure strong, consistent signal coverage, follow these guidelines:

1. Place your gateway in the centre of the network. For most devices, every time data is transmitted over one repeater hop, it loses half its speed. A central gateway minimizes the number of hops required.
2. Never go through more than three walls or floors.
3. Never go more than 50-150 feet (depending on building materials) between nodes.
4. Install no more than about five repeaters to every one gateway.

Once all nodes are plugged in, you should see them turn green on the CloudTrax Network Status page in about 5 to 15 minutes.

Allow some 20 minutes; after that time you should see the routes in the Chillifire Control panel's Router Status screen. The system automatically registers all mesh nodes against the account or sub-account you entered in the NASID field on the SSID #1 tab.